UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,281	07/25/2003	Anne Kirsten Eisentraeger	MS1-1275US	4249

22801 7590 04/09/2007
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
HO, THOMAS M	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/09/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/09/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/627,281	EISENTRAEGER ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/17/07, 3/22/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-44 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1-30 of the claimed invention is directed to non-statutory subject matter. Claims 1-17 appear to merely recite the determination of pairings for use in an elliptic curve cryptography system. In order to satisfy the requirements of 35 USC 101, the claim must result in an output towards effecting a change to a system in order to be concrete, useful, and tangible and fall within one of the statutory subclasses.

Claims 18-30 are rejected because they are not concrete, useful, and tangible in view of the disclosure within the specification (pages 31, line 10- page 32, line 6) that its implementation can be performed solely by carrier wave mediums. In order to satisfy the requirements of 35 USC 101, the claim must result in an output towards effecting a change to a system in order to be concrete, useful, and tangible and fall within one of the statutory subclasses.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-44 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. The subject matter pertaining to how the pairings are employed towards the implementation of the elliptic curve cryptography system is not disclosed.

Although breadth of claim is not per se equivalent to indefiniteness, the claims must nevertheless allow one of ordinary skill in the art to make the invention. The claims merely recite the determination of the pairings. There is no disclosure as to how the pairings are derived or determined. There is furthermore no disclosure as to how the pairings are employed in the cryptographic system.

Thus, the process in which the curves or pairings are determined, and their use in the cryptographic process, critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

Claims 4,6, 11-17, 20, 24- 30, 34, 38-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In particular, claims 13, 15, 17, 26, 28, 30, 40, 42, 44 are rejected for reciting a point Q, as **Q** and **–Q**. The Examiner is uncertain Q stores a particular point. Is Q a computer variable or a mathematical conceptual construct? Is Q a combination of two numbers when placed across a Cartesian plane, map to a particular point? Does this still apply considering the space is not a Cartesian plane, but rather within a Galois field? Is Q a vector? Does negative Q imply a scalar multiplication of –1 performed on two points? Is the space larger than two points?

Claims 11, 24, 38 are rejected for the same reasons as claim 13 for reciting a "multiple of a point".

In particular claims 12, 14, 16, 25, 27, 29, 39, 41, 43 are rejected for the similar ambiguities for a point P on elliptic curve E as to claims 13, 15, 17, 26, 28, 30, 40, 42, 44, and are further rejected because it is uncertain what j, k, the parabolic function, lambda, and the subscripted variables refer to.

For example, claim 12 recites: $f_{j,p}$ and $f_{k,P}$. Does this mean that f is a function of two variables? If so, how does a point P, presumably a dual value, and presumably a singular value j or k combine in such a function?

Lowercase j and k are undefined variables and are indefinite for this reason. Furthermore, lowercase j and k and point P, and how they relate with function f is undefined. The Examiner is uncertain if these variables are arguments to the function or serve with some other association.

Additionally, claim 12 introduces two more variables without clarification, lowercase x, lowercase y, and its subscripted variables x_4 y_4. These variables are undefined and consequently indefinite in the context of their usage.

Furthermore, their related variables x_4 y_4 are also indefinite for being undefined.

Claim 14 further recites the usage of a variable lambda which is also undefined.

Moreover the function of the parabola is undefined because in claim 12, it is referred to without being explicitly defined. In claim 14, it is undefined, because it is defined in terms of variables whose values and meanings are also undefined.

Finally, as yet a further request of clarification, the Examiner has noted that claim 12 recites "f of 2j+k, P(x) =..." while in claim 14, the parab function is defined in terms of ":="

The Examiner notes that mathematically and to those of ordinary skill in the art of computer science, there is a difference between ":=" and "="

Because the applicant has distinguished between the two assignment operators, the Applicant is asked to clarify whether the "=" used in claim 12 is an equality operator or an assignment operator.

The Examiner also requests that the Applicant clarify if the recognized assignment operator ":=" refers to a singular assignment. (ie assigning a value to a variable) or a mathematical assignment such as f(x) = y^2 which would imply a continuous assignment of values that is placed over a given domain.

Additionally, the Examiner requests that this distinction be made with regards to which functions are mathematical determinations, and which functions refer to a computer determination. For example, the input of a function with a point P for a computer function would not be indefinite. It is well known that a function may receive an abstract data type containing therein a point to be processed. However for a mathematical function or determination, it would be indefinite. One of ordinary skill in the art would expect a singular variable to refer to a singular value. One instance of F(x) = x^2 would be f(2) = 4. This is because the expected domain of X is over all real numbers.

That is not to say that other types of values may not be put into mathematical functions. However, specialized inputs in the context of mathematical determinations would require an additional introduction to inform one of ordinary skill in the art that the domain would not be over the set of real numbers, but another Applicant defined number space.

Finally, the Examiner is aware of the mathematical determinations to be made for an elliptic curve cryptography system. However, when the claims recite a determination to be made to satisfy a given equality, inequality, or property, the Applicant needs to define the space or the domain of which the determination is to be made. In the case of ECC cryptography, the attributes of the finite field and the elliptic curve must be defined.

In reference to claims 4, 6, 20, 34

The Examiner is uncertain what is referred to by the term Squared Tate pairings and squared Weil pairings.

For example, those of ordinary skill in the art understand a Weil pairing to be as follows:

Weil pairing

From Wikipedia, the free encyclopedia

Jump to: navigation, search

In mathematics, the **Weil pairing** is a construction of roots of unity by means of functions on an elliptic curve E, in such a way as to constitute a pairing (bilinear form, though with multiplicative notation) on the torsion subgroup of E. The name is for André Weil, who gave an abstract algebraic definition; the corresponding results for elliptic functions were known, and can be expressed simply by use of the Weierstrass sigma function.

Suppose E is defined over a field K. Given an integer $n > 0$ (We require n to be prime to char(K) if char(K)> 0) and suppose that K contains a primitive nth root of unity. Then the n-torsion on E has known structure, as a Cartesian product of two cyclic groups of order n. The basis of the construction is of an n-th root of unity

$$w(P,Q)$$

for given points P and Q of order n on E, by means of Kummer theory.

By a direct argument one can define a function F in the function field of E over the algebraic closure of K, by its divisor:

$$(F) = \Sigma\,(P + kQ) - \Sigma\,(kQ)$$

with sums for $0 \leq k < n$. In words F has a simple zero at each point $P + kQ$, and a simple pole at each point kQ. Then F is well-defined up to multiplication by a constant. If G is the translation of F by Q, then by construction G has the same divisor. One can show that

$$G/F \neq 1.$$

In fact then G/F would yield a function on the isogenous curve E/C where C is the cyclic subgroup generated by Q, having just one simple pole. Such a function cannot exist, as follows by proving the residue at the pole is zero, a contradiction.
Therefore if we define

$$w(P,Q) = G/F$$

we shall have an n-th root of unity (translating n times must give 1) other than 1. With this definition it can be shown that w is antisymmetric and bilinear, giving rise to a non-degenerate pairing on the n-torsion.
The Weil pairing is used in number theory and algebraic geometry, and has also been applied in elliptic curve cryptography and identity based encryption.

As the Weil pairing is a construction of roots of unity on an Elliptic curve E, and expressable by a WeierStrass Sigma function, the Examiner requests the Applicant clarify the meaning of the term Squared Weil and Tate Pairing.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1,2, 3, 5, 7, 8, 9,10, 18, 19, 21, 22, 23, 31, 32, 33, 35, 36, 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Lenstra, US patent 6446205.

In reference to claim 1:

Lenstra discloses a method for use in curve-based cryptographic logic, the method comprising:

- Determining at least one curve for use in cryptographically processing selected information, where the participant chooses a curve for use in the cryptosystem (Column 3, lines 14-20)
- Determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve, where the parabola is an elliptic curve, and wherein the pairings are sets of elliptic curve equations. (Column 3, lines 14-20) & (Column 3, lines 30 – Column 4, line 43)

In reference to claim 2:

Lenstra (Column 3, lines 15-67) discloses the method as recited in claim 1, wherein said at least one curve includes an elliptic curve. (Column 3, lines 50-53)

In reference to claim 3:

Lenstra discloses the method as recited in claim 1, wherein said pairings include Weil pairings. (Column 4, lines 35-45)

In reference to claim 5:

Lenstra discloses the method as recited in claim 1, wherein said pairings include Tate pairings. (Column 4, lines 35-45)

In reference to claim 7:

Lenstra discloses the method as recited in claim 1, further comprising:

Cryptographically processing said selected information based on said pairings. (Column 6, lines 60 – Column 7,lines 20) where the curves are selected for the ECC system (Column 3, lines 15-55) & (Figure 4)

In reference to claim 8:

Lenstra (Figure 4) & (Column 6, lines 60 – Column 7,lines 20) discloses the method as recited in claim 7, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

In reference to claim 9:

Lenstra (Figure 4) & (Column 6, lines 60 – Column 7,lines 20) discloses the method as recited in claim 7, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

In reference to claim 10:

Lenstra (Figure 4) & (Column 6, lines 60 – Column 7,lines 20) discloses discloses the method as recited in claim 7, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity based encryption process, a product identification (ID)-based process, and a short signature –based process, where the process is a key based process and an identity based encrypted process, and a short signature based process. (Column 6, lines 1-35)

Claim 18 is rejected for the same reasons as claim 1.

Claim 19 is rejected for the same reasons as claim 2.

Claim 21 is rejected for the same reasons as claim 8.

Claim 22 is rejected for the same reasons as claim 9.

Claim 23 is rejected for the same reasons as claim 10.

Claim 31 is rejected for the same reasons as claim 1.

Claim 32 is rejected for the same reasons as claim 2.

Claim 33 is rejected for the same reasons as claim 8.

Claim 35 is rejected for the same reasons as claim 8.

Claim 36 is rejected for the same reasons as claim 9.

Claim 37 is rejected for the same reasons as claim 10.

Conclusion

8. The following art not relied upon is made of record:

- US patent 5272755 discloses another elliptic curve cryptosystem.

9. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

March 31st, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100